Department of Homeland Security Daily Open Source Infrastructure Report for 24 April 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Transportation Security Administration issued a security advisory on Thursday, April 20, saying that, on April 13, 2006, a message posted in Arabic on a Web forum explained how to identify private American jets and urged Muslims to destroy all such aircraft. (See item 21)
- The Associated Press reports five teenage boys fully intended to go on a shooting spree on the anniversary of the Columbine massacre, at their Riverton, Kansas, high school but were stopped after one of them discussed the plot on a Website. (See item 46)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 24, Associated Press* — **NRC to question Pennsylvania company over stolen radioactive device.** The Nuclear Regulatory Commission (NRC) will conduct interviews into two possible violations of federal regulations stemming from the theft of a nuclear gauge from the parking lot of a motel in September. The agency said the forthcoming interviews with representatives of GeoMechanics Inc. will focus on an employee's apparent failure to properly secure the device, and the company's failure to file a written report within 30 days of the theft. The device and its case were chained to the bed of a truck that was parked at a South Charleston, WV, motel on Sunday, September 18. The gauge was found five days later along a

highway near Danville, about 28 miles away. The gauge, which contains radioactive materials americium−241 and cesium−137, is used to measure soil density. Although the company notified the NRC of the theft the day after it was stolen, it did not submit a written report until Monday, February 6.
Source: http://www.phillyburbs.com/pb−dyn/news/103−04192006−643863.h tml

2. *April 21, Financial Times* — **International Energy Agency to back nuclear power study.** An expansion of civil nuclear power offers the best hope of tackling global energy insecurity, the International Energy Agency (IEA) is expected to show in a study. The IEA is looking to nuclear power to guarantee security amid growing fears about the reliability of natural gas supplies, particularly out of Iran and Russia. Fatih Birol, the IEA's chief economist, said that security of supply and climate change were the main concerns in the years ahead. The decline of gas production in North America and in the North Sea would leave Europe and many other parts of the world hostage to a shrinking number of suppliers, reducing energy security, he warned. Analysts said the IEA's study suggested backing for nuclear power was building up and could force an end to the decades of moratoriums and stalled reactor programs that followed the Chernobyl accident 20 years ago. All 26 members of the agency support the study, although their policies on nuclear power differ widely. Austria, Germany, and Ireland oppose the use of nuclear fuel, while Spain, the UK, Italy, and Sweden are reviewing whether to build new reactors.
Source: http://news.ft.com/cms/s/bbe51f1a−d0d2−11da−b160−0000779e234 0.html

3. *April 21, St. Louis Post Dispatch* — **Large Gulf oil platform will get early restart.** Shell Exploration & Production Co. said its Mars production platform will be restarted ahead of schedule. Mars is the largest Gulf production platform damaged by Hurricane Katrina. The platform represents about five percent of the Gulf's daily oil and gas production. The company said the platform construction will be completed by the end of April.
Source: http://www.stltoday.com/stltoday/business/stories.nsf/story/2EE37011ED4B4FF186257157000D2F7E?OpenDocument

4. *April 20, Houston Business Journal* — **ExxonMobil reverse−pipeline project brings Canadian oil to Texas.** For the first time, Canadian crude oil is being delivered to the Gulf Coast through a pipeline that used to flow the other direction. Mobil Pipe Line Co. successfully reversed an 858−mile, 20−inch diameter crude oil pipeline that had historically run from Nederland, TX, to Patoka, IL. Deliveries of Canadian crude to Beaumont−area refineries began in early April. The pipeline reversal project gives shippers of western Canadian crude oil direct pipeline access to U.S. Gulf Coast refining markets while also enabling Mobil Pipe Line to optimize a previously under−utilized pipeline, the company says. Canadian shippers have committed an average volume of 50,000 barrels per day for the next five years, ExxonMobil Pipeline President Mike Tudor said, and he expects that the pipeline will operate on average near its estimated capacity of 66,000 barrels per day of heavy crude.
Source: http://www.bizjournals.com/houston/stories/2006/04/17/daily4 7.html?from_rss=1

5. *April 19, Canadian Press* — **Nuclear power top option for Ontario compared to alternatives, premier says.** Nuclear power may be the best option to fulfill Ontario's future electricity needs, despite downsides including Chornobyl−type accidents and radioactive waste, Premier Dalton McGuinty said. Natural gas is too expensive, wind power is unreliable, coal

plants pollute the air and Ontario's hydroelectric potential has largely been maxed out −− leaving nuclear power expansions "on the table," McGuinty said. Energy Minister Donna Cansfield will soon issue a formal response to recommendations in December that called for $40 billion to construct or replace up to 12,400 megawatts of nuclear power in Ontario −− requiring 12 or more new nuclear reactor units in the province. Critics say there have been close calls at Ontario's nuclear stations, including two incidents at the Pickering station −− a coolant leak in 1983, and brief problems with computers that operate a reactor in 1991. The western world is largely shying away from nuclear plants with the notable exception of Finland, which is constructing a nuclear station to reduce that country's reliance on Russian gas. The government has promised to close Ontario's four remaining coal plants by the end of 2009 due to air pollution concerns.
Source: http://news.yahoo.com/s/cpress/20060419/ca_pr_on_na/ont_nucl ear_power_1

6. *April 19, Associated Press* — **Calpine closes sale of Mexican plant.** Calpine Corp. said it closed the $43 million sale of its 45 percent stake in a Mexican power plant as part of the company's restructuring plan under Chapter 11 bankruptcy protection. Calpine agreed in March to sell its interest in 525−megawatt Valladolid III Power Plant on Mexico's Yucatan Peninsula to Mitsui & Co. and Chubu Electric Power Co.
Source: http://biz.yahoo.com/ap/060419/calpine_sale.html?.v=1

[Return to top]

Chemical Industry and Hazardous Materials Sector

7. *April 21, Associated Press* — **Louisiana natural gas plant fire forces temporary evacuations.** A natural gas plant caught fire in Vermilion Parish, LA, early Friday, April 21, closing roads in the area and forcing the evacuation of residents and businesses within a one−mile radius. No injuries were reported.
Source: http://www.chron.com/disp/story.mpl/business/energy/3810175. html

8. *April 21, Access North GA* — **Tanker explosion prompts road closure in Georgia.** No one was injured in a tanker explosion Friday morning, April 21, at the corner of Georgia 400 and Georgia 60 in Lumpkin County, GA. The incident began when a motorist got distracted and rammed into the side of the tanker. Georgia 60 and Georgia 115 north of Georgia 400 were closed for hours following the accident.
Source: http://www.accessnorthga.com/news/hall/newfullstory.asp?ID=1 03170

9. *April 20, KAKE (KS)* — **Chemical mixture sparks fire, prompts road closure.** Leaking chemicals at the APEX Engineering Inc. plant in Wichita, KS, caused a scare in one neighborhood when a 920−degree mixture of sodium nitrate and potassium nitrate sparked a small fire. As a result, nearby roads were closed for much of the morning. Firefighters were able to extinguish the small fire quickly, but fixing the leak was a lengthy process.
Source: http://www.kake.com/home/headlines/2668426.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

10. *April 20, TechNewsWorld* — **Security firms identify malware−for−sale racketeers.** A malware−for−sale ring used to distribute customized copies of a data−pilfering Trojan has been cracked by two computer security firms. Panda Software and RSA Security "neutralized" several Websites that were providing information thieves with customized versions of the Briz.A Trojan, according to Panda. Panda said it intercepted information pinched by the malware, including "hundreds of user names and passwords for banks, telecommunication companies, hotels, airlines and international betting services." Panda Chief Technology Officer Patrick Hinojosa said, "From the FTP logs that we were able to see, which is where information from infected PCs came streaming in, many, many thousands of PCs were infected." However, another security firm, Islandia, N.Y.−based eTrust Security Management, discounted the breadth of the threat. The distribution of the malware was being handled like a business, Hinojosa noted. The basic Trojan was being sold for US $990. Additional modules could be purchased for tasks such as hacking servers to retrieve stolen password information and compromising FTP sites to store the ill−gotten gains. Panda and RSA were able to shut down some malignant servers, Hinojosa said, and have turned over the findings to law enforcement authorities in Russia and Eastern Europe.
Source: http://www.technewsworld.com/rsstory/50061.html

11. *April 20, CNET News* — **Man charged with hacking college database.** A 25−year−old San Diego man has been charged with hacking into the University of Southern California's (USC) online application system and nabbing personal data from prospective students. On Monday, April 17, the U.S. Attorney's Office in Los Angeles filed a criminal complaint against a network administrator, for allegedly exploiting a vulnerability in a USC database that hosts and stores student applications. Michael Zweiback, an assistant U.S. attorney in the cybercrimes and intellectual property unit, said that the case reflects a growing trend among hackers. "Universities are becoming bigger and bigger targets to the hacker community because they are large institutions..." Zweiback said. According to the complaint, McCarty allegedly used his home computer on June 17, 2005 to hack into a password−protected USC database. It contained data on more than 275,000 applicants from 1997 through that time, including Social Security numbers and birthdates. USC shut down the Website on June 21, 2005 after learning about the hack from SecurityFocus. The site was offline for two weeks. The FBI found McCarty through the Internet Protocol number on his home computer.
Source: http://news.com.com/Man+charged+with+hacking+USC+database/2100−7350_3−6063470.html?tag=cd.lede

12. *April 20, IDG News Service* — **Major banking sites insecure, researcher warns.** Many of the most popular banking sites in the U.S. may be needlessly placing their customers at risk to online thieves, a security researcher warned Thursday, April 20. At issue are the user log−in areas on sites that ask customers to submit their ID and password information. Although these

forms may be encrypted, they do not use authentication technology to prove they are genuine, according to Johannes Ullrich, chief research officer at the SANS Institute. A more secure approach would be to force users to log in on an HTTP Secure (HTTPS) Web page. HTTPS pages use the Secure Sockets Layer (SSL) security protocol, which not only encrypts the information on the page but also provides digital certificates to give assurance that the Website in question is genuine. Often banks include SSL log−in pages as an option, but they can be hard to find, Ullrich said. One trick for finding these pages, which will prompt Firefox and Internet Explorer to display a yellow lock icon on the bottom of the screen, is to submit a bad password on the home page. Often bank sites will redirect users to the SSL log−in page after that happens, he said.
Source: http://www.computerworld.com/securitytopics/security/story/0,10801,110738,00.html?SKC=security−110738

13. *April 20, Associated Press* — **Check scam out of Pizza Hut uncovered.** Police traced a check counterfeiting ring back to a suburban Memphis, TN, Pizza Hut where three suspects forged at least $60,000 worth of bad checks in four states, authorities said. The manager of the pizza restaurant in Germantown, TN, now faces a charge of identity theft trafficking for victimizing customers who paid by check, said Germantown Police Capt. Lee Covey. Police also arrested accomplices after witnessing an exchange of checking account numbers and names. The perpetrator was giving accomplices information from customers' checks and they used forged checks to purchase merchandise in Mississippi, Alabama, Louisiana, and Illinois, Covey said. Germantown Police Detective Mike Grey followed a trail of receipts to the Pizza Hut after several Germantown residents reported unauthorized purchases made from their checking accounts.
Source: http://www.knoxnews.com/kns/state/article/0,1406,KNS_348_4637136,00.html

14. *April 17, Technology Review* — **Open season on phishing.** Consumer−level security tools, such as Norton Internet Security already filter out many phishing e−mails before they arrive. But a few inevitably get through, and it's what happens after users have clicked on deceptive links and have begun to enter personal information into fraudulent websites that now concerns many security researchers. Part of the problem is that many people don't have security software on their computers, and the few existing programs that stop people from sending such information to "phishers" work only with specific browsers, such as Microsoft Internet Explorer. Now researchers at BBN Technologies are using funding from the Department of Homeland Security to develop a phishing defense that isn't keyed to specific browsers. While the project is at an early stage, BBN will provide its results later this year to collaborator Symantec, whose Norton suite of products leads the consumer computer security industry. The system works by intercepting personal information typed into a Web page before it actually leaves a user's computer; it alerts the user if the information is sensitive or if the page has been identified as part of a phishing site.
Source: http://38.113.17.100/read_article.aspx?id=16702&ch=infotech

[Return to top]

Transportation and Border Security Sector

15.

April 23, Chicago Tribune — **Flight from Chicago diverted to Denver.** A United Airlines flight from Chicago to Sacramento was diverted to Denver International Airport and the passengers evacuated when somebody claimed to have a bomb, airport officials said. It was unclear whether the person made the threat while Flight 735 was airborne or after it landed Friday afternoon, April 21, an airport spokesperson said. Authorities found nothing when bomb−sniffing dogs checked the passenger compartment and cargo area and bags were re−screened.
Source: http://www.chicagotribune.com/news/nationworld/chi−060423038 1apr23,1,5263525.story?coll=chi−newsnationworld−hed

16. *April 21, Department of Transportation* — **Louisiana receives additional $53 million to repair hurricane−damaged railroad signals and highways.** Louisiana is receiving an additional $53 million in federal funds to help restore railroad signals, clear roads and continue repairs to hurricane−damaged highways and bridges, Department of Transportation Secretary Norman Y. Mineta said on Friday, April 21. The Department has now made over $1 billion available to Louisiana with this latest round of support, Mineta added. The new funding announced reimburses the state for repairing railroad signals in Orleans, Jefferson and Plaquemines Parishes and additional expenses from clearing downed trees, sand and other debris from highways after the storm. The funding has been used to reopen the I−10 Twin Spans Bridge and repair or replace traffic signals, highway signs, guardrails and washed out pavement and highway shoulders. This funding is part of an emergency highway aid package for Gulf Coast states requested by President Bush and approved by Congress the end of last year. In addition to providing federal dollars, Mineta said the Department of Transportation has made it easier for Louisiana to use those funds by cutting red tape and giving state officials the flexibility to get repairs underway as quickly as possible.
Source: http://www.dot.gov/affairs/dot5106.htm

17. *April 21, Associated Press* — **AirTran flight from Atlanta struck by lightning.** An airplane was struck by lightning shortly after taking off but returned safely to Atlanta's Hartsfield−Jackson International Airport, authorities said. The AirTran flight, which had 116 passengers and five crewmembers, took off shortly before 10 p.m. Thursday, April 20, during a thunderstorm. It was bound for Washington, DC.
Source: http://www.usatoday.com/travel/flights/2006−04−21−lightning− flight_x.htm

18. *April 21, USA TODAY* — **Travel industry offers driver incentives.** With gas prices soaring, nervous travel companies and drive−to destinations are offering earlier−than−normal incentives to hit the road, from $20 ethanol vouchers in South Dakota to discounts of $10 per car−engine cylinder at bed−and−breakfast inns in Maine. Surveys released this week by the American Petroleum Institute and U.S. Energy Information Administration showed that Americans have curbed their gas use in apparent response to higher prices at the pump. Last month, 68 percent of vacationers polled by the motorist group AAA said they would consider reducing the number of driving trips if the average price of regular unleaded gas topped $2.85 a gallon −− with that number climbing to 83 percent if the price reaches $3.35 a gallon. Thursday's nationwide average was $2.83, up 61 cents from a year ago, AAA reports. Average per−gallon prices for regular unleaded already straddle $3 in California, Hawaii, New York and Washington, D.C., and have reached $3.60 a gallon in Canada. And with oil prices spiking to a new high of $74 a barrel Thursday, gas watchers say the worst may be yet to come.

Source: http://www.usatoday.com/travel/destinations/2006−04−20−gas−p rices_x.htm

19. *April 21, Associated Press* — **Airlines buffeted by revenue gains, higher fuel costs.** Travelers are boarding planes in increasing numbers and are paying more for tickets, boosting revenue at U.S. airlines, but the carriers continue to struggle with jet fuel prices that could be headed even higher. Southwest Airlines, Continental Airlines and Alaska Air Group all said on Thursday, April 20, that their first−quarter revenue jumped by double−digit amounts, but only Southwest earned a profit. Airline executives worry whether consumers facing $3 a gallon gasoline and higher utility bills will have enough left over to take airplane trips, especially with airfares rising. Earlier this week, American Airlines added $10 to its leisure fares, a move that was quickly matched by most other major carriers. There have been more than a dozen increases since the beginning of last year, driving up prices on some routes more than 50 percent. Helane Becker, an analyst with The Benchmark Co., predicted that the airlines will have a strong summer travel season despite the higher prices. But, she said, doubts are growing about the second half of the year. "If oil prices stay high, and people with big SUVs are paying $100 to fill their tank, anybody who hasn't already planned a vacation probably won't go," Becker said.
Source: http://www.usatoday.com/travel/flights/2006−04−21−airline−ea rnings_x.htm

20. *April 21, Associated Press* — **Delta says airport security snafu cost it $1.3 million.** Delta Air Lines Inc., which is operating under bankruptcy protection, said Friday, April 21, a computer software glitch at a security checkpoint at the world's busiest airport cost it more than $1.3 million. The revelation about Wednesday's disruption, April 19, at Hartsfield−Jackson Atlanta International Airport came in a letter from Joe Kolshak, Delta's executive vice president and chief of operations, to Transportation Security Administration Director Kip Hawley. "These costs are not insignificant for an airline that is fighting for its survival," Kolshak wrote. Hawley told reporters Thursday that the scare that shut down security checkpoints for two hours was the result of a computer glitch in testing software. He said an airport screener spotted what looked like an explosive on an X−ray machine. She pressed a button that should have signaled a routine security test was being conducted but it failed to respond, Hawley said. By the time checkpoints reopened, no planes had departed for more than an hour and all arrivals were delayed by at least 90 minutes. The shutdown came at peak travel time and at least 120 flights were affected. Kolshak said that more than 7,000 Delta customers were affected by flight cancellations, diversions and delays.
Source: http://www.macon.com/mld/macon/news/politics/14399445.htm

21. *April 21, Transportation Security Administration* — **Transportation Security Administration has issued a security advisory.** The Transportation Security Administration (TSA) issued a security advisory on Thursday, April 20, saying that, on April 13, 2006, a message posted in Arabic on a Web forum explained how to identify private American jets and urged Muslims to destroy all such aircraft: “Destroy private American aircraft…We call upon all Muslims to follow and identify private civilian American aircrafts in all airports of the world…It is the duty of Muslims to destroy all types of private American aircrafts that are of the types Gulf Stream and Lear Jet and all small jet aircraft usually used by distinguished (people) and businessmen.” The message also advised readers how to identify American aircraft and provided the tail number of a private aircraft allegedly used by the CIA. The advisory also said that the theft of any General Aviation aircraft should be immediately reported to the appropriate authorities and the TSA General Aviation Hotline at 866−GASECUR (866−427−3287).

Transportation Security Administration: http://www.tsa.gov
Source: http://web.nbaa.org/public/ops/security/DHSAdvisory20060420. pdf

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

22. *April 21, Advocate (LA)* — **Agriculture production drops.** The overall value of Louisiana's agricultural production dropped by one billion dollars in 2005 because of hurricanes Katrina and Rita, and Louisiana State University (LSU) officials warned the long−term effects of the storms could continue to hurt the farm economy. Paul Coreil, vice chancellor of the LSU Agricultural Center, said Katrina and Rita caused tremendous hardships to Louisiana farmers, foresters, fishermen and cattlemen, but some crops weren't affected because harvests had been completed before the hurricanes. "Future production will suffer from the consequences of saltwater intrusion, animal losses and an infrastructure that's still under repair," Coreil said. For 2005, the agricultural center estimated the gross farm income from plant, animal, fisheries and wildlife commodities produced in Louisiana totaled $4.69 billion. The economic value added through processing, marketing and transportation of those commodities totaled $5.05 billion −— bringing the estimate of Louisiana's total economic value of agriculture to $9.74 billion last year. That's down from a five−year peak of $10.7 billion in 2004.
Louisiana Summary of Agriculture and Natural Resources for 2005:
http://www.lsuagcenter.com/agsummary/
Source: http://www.2theadvocate.com/news/2670006.html

23. *April 20, Associated Press* — **Brazil detects new foot−and−mouth outbreak.** Brazil's Agriculture Ministry on Thursday, April 20, confirmed an outbreak of foot−and−mouth disease (FMD) on a farm in Mato Grosso do Sul, the country's biggest cattle state, near the Paraguay border. The new case of the highly contagious disease was discovered at the Sitio Medianeira in Japora, one of three districts sealed off after FMD was reported last October. The ministry said in a statement the farm's entire herd of 137 cows will be slaughtered, although blood tests showed that only 22 were infected. The herd had last been vaccinated against the disease in May 2005.
Source: http://www.alertnet.org/thenews/newsdesk/N20313898.htm

[Return to top]

Food Sector

24. *April 21, Reuters* — **Japan consumers voice U.S. beef worries at meeting.** Japanese consumers voiced concerns about a U.S. inspection system for mad cow disease at a meeting in Tokyo on Friday, April 21, sponsored by the government to discuss a resumption of U.S. beef

imports. It was one of 10 meetings on the issue across the nation at which government officials explained steps the U.S. had promised to take not to repeat a violation of export conditions agreed by the two nations to ensure the safety of U.S. beef. Japan suspended U.S. beef imports on January 20, just a month after it partially lifted a two−year−old ban on U.S. beef imposed over mad cow disease fears, when Japanese inspectors discovered banned spinal material in a veal shipment from New York. The government has said that for an import resumption, it is vital to dispel doubts over confidence in the export system.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/21/AR2006042100314.html

25. *April 20, Associated Press* — **Poultry worker opens fire at Arkansas plant.** A Tyson Foods Inc. employee who had just been suspended from his job returned to the poultry processing plant carrying two pistols and opened fire, wounding a co−worker before police shot the gunman, officials said. The worker had been escorted out of the plant Wednesday, April 19, but reappeared later that night with weapons, Tyson spokesperson Gary Mickelson said. Between 400 and 500 people were evacuated from the plant.
Source: http://www.chron.com/disp/story.mpl/ap/nation/3808872.html

[Return to top]

Water Sector

26. *April 21, Daily News (LA)* — **Drought grips Louisiana.** Much of South Louisiana is in the midst of a drought that has lasted more than a year. According to the most recent precipitation reports from the state office of climatology, only the areas in the northern part of the state have met the year−to−date rainfall norms through April 9. Statewide, the year−to−date average is 12.18 inches against a norm of 17.36 inches. The average for the past four weeks is 2.38 inches with 14 of the 33 reporting stations recording less than three−quarters−inch over the past month. "Parts of the state have been suffering for quite some time," said Jay Grymes, LSU AgCenter climatologist. "In the southern third of Louisiana, the dry spell goes back to the beginnings of 2005, and even sections of northern Louisiana have been dealing with dry weather over the past 12 to 15 months." Grymes said that in Baton Rouge, 12 of the past 14 months have had below−normal rainfall. The only two exceptions were August and September, which correspond to hurricanes Katrina and Rita. Much of south−central and southeastern Louisiana is showing a similar drought trend for the past year.
Source: http://www.edailynews.info/articles/2006/04/21/news/news01.t xt

[Return to top]

Public Health Sector

27. *April 21, Agence France−Presse* — **Two new cases of bird flu in France.** Two new cases of the H5N1 strain of bird flu have been detected in two wild swans found dead the week of April 17 in the center−east of France, the agriculture ministry revealed. The dead birds were discovered in marshland in the Ain region where all but one of the bird flu cases recorded in the country have come from. Since the beginning of the year, and including the latest cases, 64 wild

birds have been found with H5N1 in France. Sixty−three were in the Ain region and one was foun in the southeastern Bouches−du−Rhone region, according to a ministry statement. A total of 14,000 birds have been tested.
Source: http://news.yahoo.com/s/afp/20060421/hl_afp/healthflufrance_060421122910

28. *April 20, Associated Press* — **Iowa plans mass mumps vaccinations.** Mass clinics for mumps immunization will open for young adults next week in Iowa, the state at the center of a regional epidemic, health officials said Thursday, April 20. The state will target 18 to 22−year−olds, dividing 25,000 doses among counties with colleges, universities and post−secondary institutions, where students are especially vulnerable to contracting and spreading the virus, said Mary Mincer Hansen, Iowa public health director. The mumps outbreak is being called the nation's worst in 20 years. As of Thursday, Iowa had 975 cases of probable, confirmed and suspected cases, said Patricia Quinlisk, the state epidemiologist.
Mumps information: http://www.cdc.gov/nip/diseases/mumps/default.htm
Source: http://abcnews.go.com/Health/wireStory?id=1866736

29. *April 20, Agence France−Presse* — **Bird flu scare quarantines plane in Denmark.** Copenhagen airport quarantined an aircraft due to fears that a passenger had contracted the H5N1 bird flu virus, but her ailment turned out to be a stomach bug, airport police said. Prior to landing the captain of an incoming Singapore Airlines aircraft warned Danish authorities that a passenger showed possible bird flu symptoms. The aircraft with 275 passengers and 20 crew on board was directed to an isolation area at Kastrup airport. A medical team established that the traveler in question, a 31−year−old Swedish woman, was simply suffering from an upset stomach.
Source: http://news.yahoo.com/s/afp/20060420/hl_afp/healthfludenmark_060420202054;_ylt=AhsXKRVaHzOxOO1XCkNzmZqJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

30. *April 20, Georgia Institute of Technology* — **Program to halt pandemics installed in Georgia.** Researchers at the Georgia Institute of Technology have developed a computer program, based on a clinical model created by the U.S. Centers for Disease Control and Prevention, to help state, city and county health care departments create and test more efficient plans for treating infectious illness. The program, called RealOpt, will be installed over the next few months at health departments across the state of Georgia and health departments in 35 other states have plans to test the program. While the program is still in the testing phase, it will soon be available free to any government health department that requests it. RealOpt takes the numerous variables associated with a health care department’s treatment of a very large group of people, and through large−scale simulation and optimization pinpoints the most efficient way to move patients to and through a facility. Using the program, a health care department can determine the best location for emergency clinics based on population density and road accessibility, the most efficient facility layout, the number of health care professionals needed in certain areas, the number of vaccinations needed and the time it will take to treat patients.
Source: http://www.gatech.edu/news−room/release.php?id=941

[Return to top]

Government Sector

31. *April 21, Associated Press* — **Air Force One subject of Internet hoax.** A startling Internet video that shows someone spraying graffiti on President Bush's jet looked so authentic that the Air Force wasn't immediately certain whether the plane had been targeted. It was all a hoax. No one actually sprayed the slogan "Still Free" on the cowling of Air Force One. The pranksters responsible for the grainy, two−minute Web video −− employed by a New York fashion company −− revealed Friday, April 21, how they pulled it off: a rented 747 in California painted to look almost exactly like Air Force One. The video shows hooded graffiti artists climbing barbed−wire fences and sneaking past guards with dogs to approach the jumbo jet. They spray−paint a slogan associated with free expression. After the video began circulating on the Web on Tuesday, the Air Force checked to see whether the plane had been vandalized. Lt. Col. Bruce Alexander, a spokesperson for the Air Mobility Command's 89th Airlift Wing, which operates Air Force One, later confirmed that no such spray−painting had occurred.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=48719

[Return to top]

Emergency Services Sector

32. *April 20, Federal Computer Week* — **FEMA working on business relationships.** The Federal Emergency Management Agency (FEMA) is making sure proper business relationships are in place before it responds to this year's hurricane season, the agency's new deputy director of operations, Deidre Lee, said Thursday, April 20. Congress and the public berated FEMA last year after the agency spent millions of dollars on last−minute hurricane relief deals that yielded few results. "We have renewed focus to ensure we get it right," said Lee. FEMA is emulating the Department of Defense in establishing business relationships before crises occur, she said.
Source: http://www.fcw.com/article94137−04−20−06−Web

33. *April 20, St. Paul Pioneer Press (MN)* — **In once−rural landscapes, emergency planners scramble to extend siren coverage.** If tornados touch down in the eastern portion of the Minneapolis or St. Paul, MN, tens of thousands of residents in fast−growing suburbs may not hear the warning sirens. Once−rural landscapes used to be so sparsely populated that an outdoor warning system couldn't be justified. But in recent years, housing developments have exploded beyond the sirens' range −− and local emergency planners are scrambling to keep up. A Pioneer Press analysis of siren locations in Ramsey, Dakota, Washington and Anoka counties indicate about 200,000 people may be out of earshot. Many live in the newest areas of a city, and others are in the subdivisions that quickly are replacing farm fields in unincorporated areas. "It's a deep concern," said Tom Cherney, the state's former Department of Homeland Security communications and warnings officer. "There are holes in the system." Forest Lake Council Member Rick Ashbach, who served previously on the town board, called the lack of sirens "a failure from the standpoint of emergency management." Ashbach said the city is working to correct the problem as they continue to add sirens. Fire Chief Sigfrinius said, however, he had no idea when the eastern portion of the city might be covered.
Source: http://www.twincities.com/mld/pioneerpress/news/local/143820 45.htm

34. *April 20, Fort Bend Herald (TX)* — **Drill conducted in Texas to test debris removal and communication with public.** Fort Bend County, TX, and local city officials on Wednesday,

April 19, practiced their response to a major hurricane. Fort Bend County Emergency Coordinator Jeff Braun said the exercise tested the ability of local officials to not only communicate among themselves, but also with the greater community. This year's drill examined how county and city officials would react to a hurricane that touched down near Fort Bend County, and has just passed through. The drill examined aspects of debris removal and communication with the public. Over 200 people participated. Participants said they were not familiar with the county's emergency management software and technology, and monthly training sessions were suggested as a result.
Source: http://www.herald−coaster.com/articles/2006/04/20/news/news0 2.txt

35. *April 20, Clayton News Daily (GA)* — **Airport hosts mock disaster.** There was something amiss on BWA Flight 1388, bound from Europe to Hartsfield−Jackson Atlanta, GA, International Airport. At least, that's what the scenario was for the "Big Bird 2006" safety drill at the airport on Thursday, April 20, according to Hartsfield−Jackson Deputy Fire Chief Harold Miller. This exercise was intended to test a quarantine procedure that airport officials began to develop in 2002 when there was concern about the use of smallpox in a terrorist attack. "Now we have a procedure that will work for any communicable disease," Miller said. That procedure has been "table−top tested," but Thursday was the first time all of the players were brought together to implement the plan in a real−world situation. Along with the airport's fire fighting unit, which is part of the City of Atlanta Fire Department, some of the participating agencies included the Centers for Disease Control and Prevention, U.S. Customs and Border Protection, the American Red Cross.
Source: http://www.news−daily.com/homepage/local_story_110230802.htm l?keyword=leadpicturestory

36. *April 20, KTRK (TX)* — **Big changes coming to Texas evacuation plan.** The changes in the Texas evacuation plan are designed to correct the mistakes made during Hurricane Rita. For the first time, contra flow is part of a regional evacuation plan. The order to institute contra flow would come from the Department of Public Safety. The Texas Department of Transportation would implement it. In addition, the state will contract with wrecker services to remove disabled vehicles from highways. As for the gas shortage seen in Rita, a state fuel desk will be activated in Austin. Gas stations will be asked to remain open. Fuel trucks will be brought in before an evacuation and posted along routes. There will also be state−positioned aid stations along evacuation corridors, providing water and restrooms.
Source: http://abclocal.go.com/ktrk/story?section=local&id=4101865

[Return to top]

Information Technology and Telecommunications Sector

37. *April 21, Register (UK)* — **China poised to pinch U.S. spam crown.** China is closing in on the U.S. at the top of a league of spam relaying countries. According to statistics from security firm Sophos, China originated 21.9 percent of the junk mail messages captured in its spam traps compared to 23.1 percent for the U.S. Two years ago, the U.S. accounted for half of all spam sent in the world, a figure that has now dropped to less than a quarter, thanks to crackdowns against spammers and better information sharing among ISPs.
Source: http://www.channelregister.co.uk/2006/04/21/spam_relay_hotli st/

38. *April 21, Xinhua (China)* — **HP recalls 15,700 laptop batteries due to fire hazard.** For the second time in six months Hewlett Packard (HP) has issued a worldwide recall on Thursday, April 20, for 15,700 laptop China−made batteries which can pose potential fire hazard because of overheating. The recall is for lithium ion rechargeable batteries manufactured in early January 2005 and used with various HP and Compaq computers. The affected batteries have a bar code label starting with L3, the agency said.
Source: http://news.xinhuanet.com/english/2006−04/21/content_4455781 .htm

39. *April 20, Security Focus* — **Apple Mac OS X multiple security vulnerabilities.** Apple Mac OS X is reported prone to multiple security vulnerabilities. Analysis: BOMArchiveHelper is the default archive file handler in Mac OS X. It runs as a service that does not have a GUI interface. It is invoked when double clicking on a archived file. A heap overflow vulnerability exists within BOMArchiveHelper which allows for an attacker to cause the application to crash, and or to execute arbitrary code on a targeted host. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17634/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/17634/references

40. *April 20, Security Focus* — **Linksys RT31P2 remote malformed SIP packet denial−of−service vulnerabilities.** Linksys RT31P2 routers are susceptible to multiple remote denial−of−service vulnerabilities because the devices fail to properly handle malformed network traffic. Analysis: A remote, unauthenticated attacker may be able to cause a denial−of−service condition. For example, when the phone is being used off hook, an attacker may be able to disrupt the call. When the phone is not being used on hook, an attacker may be able to cause the phone to stop working. Vulnerable: Linksys RT31P2 VoIP Router 0.
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for these issues.
Source: http://www.securityfocus.com/bid/17631/references

41. *April 20, Information Week* — **Oracle bug exploit loose.** An exploit that leverages one of the three dozen vulnerabilities patched Tuesday, April 18, by Oracle has been spotted in the wild, a security company said Thursday, April 20, making patching even more essential. According to an alert sent by Symantec to customers of its DeepSight system, an exploit for one of the Oracle flaws was published on the Bugtraq security mailing list. The exploit, which targets one of the Oracle Database 10g bugs, escalates privileges of existing users to give them total access to the database. Installing the available patch is critical, security experts say.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=186500325

42. *April 20, Computer World* — **Linux desktop growth could spur new malware activity.** Besides Linux's low cost, its relative immunity from viruses, spyware, worms and other malware has long been one of the open−source operating system's key attractions to potential desktop users. But experts warn that could change if Linux begins to win a mass audience on the desktop, bringing in millions of users who are less proficient technically and less security−conscious than today's typical Linux user. The number of viruses that has so far targeted Linux remains small compared with the thousands of viruses and billions of dollars in estimated damage and lost productivity caused by Windows viruses. Some experts argue that

because Linux, with its Unix heritage, was created from the ground up as a multi−user system with built−in access controls and privileges, it is fundamentally more secure than Windows. The relatively small number of Linux users spread among different versions of Linux has long hindered the growth of new software by creating a lower reward/effort ratio. That has also driven away virus creators, said Ed Metcalf, product marketing manager at McAfee Inc. Regardless, some Linux users, while reluctant to install antivirus software on client computers, are starting to take more safety measures.
Source: http://www.computerworld.com/softwaretopics/os/linux/story/0 ,10801,110710,00.html

43. *April 20, Tech Web* — **Microsoft patch 'erases' Outlook Express addresses.** Another Microsoft patch from the batch released last week is apparently causing problems, at least according to numerous Windows users on the Redmond, WA, developer's official message boards. After applying the patch from security bulletin MS06−016, say dozens of users, their Outlook Express e−mail client's address book disappeared and form−style messages can't be sent. The problem said users, including several Microsoft MVPs, was the MS06−016 patch (also tagged as KB911567). Uninstalling the patch returned the address book to its prior state and allowed template−based messages to be e−mailed normally.
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=SSYKRYB5EYMMKQSNDBGCKHSCJUMEKJVN?articleID=186500318

44. *April 19, Security Tracker* — **CiscoWorks Wireless LAN Solution Engine cross site scripting flaw.** A vulnerability was reported in the CiscoWorks Wireless LAN Solution Engine (WLSE) software. A remote user can conduct cross site scripting attacks to gain administrative access. Analysis: The WLSE Web interface does not properly filter HTML code from user supplied input before displaying the input. A remote user can cause arbitrary scripting code to be executed by the target administrator's browser. The code will originate from the WLSE appliance and will run in the security context of that interface. As a result, the code will be able to access the target administrator's cookies including authentication cookies, if any, associated with the interface, access data recently submitted by the target administrator via Web form to the interface, or take actions on the interface acting as the target administrator. Affected version(s): prior to 2.13.
Solution: Cisco has issued a fixed version (2.13), available at:
http://www.cisco.com/cgi−bin/tablebuild.pl/wlan−sol−eng
The Cisco Security Advisory is available at:
http://www.cisco.com/warp/public/707/cisco−sa−20060419−wlse. shtml
Source: http://securitytracker.com/alerts/2006/Apr/1015965.html

45. *April 19, Tech Web* — **Mobile browsing seen changing face of Web.** People are turning to mobile phones for Internet use more quickly than they are adopting laptops for the same purpose in many parts of the world, according to a recent study of Internet trends. Personal computers are still the most popular way to gain Internet access, but the rapid pace of mobile phone installation and the development of wireless networks is driving robust growth in the use of phones for browsing, according to results from The Face of the Web, an annual study by Ipsos Insight. Applications are expected to grow and mobile phones are poised to overtake the personal computer as the dominant Internet platform in some markets.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=186100308

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code and materials explaining how to exploit a race condition vulnerability in Sendmail. Sendmail improperly handles asynchronous signals causing a race condition vulnerability. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user. For more information please review the following:

TA06−081A − Sendmail Race Condition Vulnerability
http://www.us−cert.gov/cas/techalerts/TA06−081A.html

VU#834865 − Sendmail contains a race condition
http://www.kb.cert.org/vuls/id/834865

Sendmail MTA Security Vulnerability Advisory
http://www.sendmail.com/company/advisory/

US−CERT recommends the following actions to mitigate the security risks:

Upgrade to the latest version: Sendmail 8.13.6.
http://www.sendmail.org/releases/8.13.6.html

Review the Sendmail MTA Security Vulnerability Advisory for steps to reduce the impact of this vulnerability. http://www.sendmail.com/company/advisory/#mitigation

US−CERT is not aware of any working exploit code at this time.

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 50497 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 80 (www), 32459 (−−−), 1197 (−−−), 56431

	(−−−), 1434 (ms−sql−m), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

46. *April 21, Associated Press* — **Kansas teens accused of Columbine−style plot.** Five teenage boys fully intended to go on a shooting spree at their Riverton, KS, high school but were stopped after one of them discussed the plot on a Website, law enforcement and school officials said. The boys, ranging in age from 16 to 18, were arrested Thursday, April 20, the anniversary of the Columbine massacre, just hours before they planned to shoot fellow students and school employees, authorities said. "What the resounding theme is: They were actually going to do this," Cherokee County Sheriff Steve Norman said. The teens planned to wear black trench coats and disable the school's camera system before starting the attack between noon and 1 p.m. CDT Thursday, Norman said. Sheriff's deputies found guns, ammunition, knives, and coded messages in the bedroom of one suspect and documents about firearms and references to Armageddon in two suspects' school lockers. Norman said school officials began investigating Tuesday, April 18, after learning a threatening message had been posted on MySpace.com. Four of the suspects were arrested at their homes; the fifth was taken into custody at the school. Riverton is a small community of about 600 people along what once was the famed Route 66 in southeast Kansas, near the Oklahoma and Missouri borders.
Source: http://www.cnn.com/2006/US/04/21/foiled.plot.ap/index.html

[Return to top]

General Sector

47. *April 21, Associated Press* — **Two Atlanta−area men plotted terrorist attacks, FBI says.** A 21−year−old Georgia Tech student and another man traveled to Canada to meet with Islamic extremists to discuss "strategic locations in the United States suitable for a terrorist strike," according to an affidavit made public Friday, April 21. Syed Haris Ahmed and Ehsanul Islam Sadequee, both U.S. citizens who grew up in the Atlanta area, met with at least three other targets of ongoing FBI terrorism investigations during a trip to Canada in March 2005, an FBI agent's affidavit said. The affidavit said the men discussed attacks against oil refineries and military bases and planned to travel to Pakistan to get military training at a terrorist camp, which authorities said Ahmed then tried to do. Ahmed, who was indicted on suspicion of giving material support to terrorism, was being held at an undisclosed location. Sadequee, 19, who is accused of making materially false statements in connection with an ongoing federal terrorism investigation, was arrested in Bangladesh and was en route to New York City to be arraigned. "There is no imminent threat," said FBI Special Agent Richard Kolko, a spokesperson in Washington.
Source: http://www.accessnorthga.com/news/ap_newfullstory.asp?ID=743 21

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer